Deutscher Bundestag **Drucksache 17/6825**

17. Wahlperiode 18. 08. 2011

Kleine Anfrage

der Abgeordneten Agnes Malczak, Omid Nouripour, Tom Koenigs, Dr. Konstantin von Notz, Marieluise Beck (Bremen), Volker Beck (Köln), Viola von Cramon-Taubadel, Thilo Hoppe, Uwe Kekeritz, Katja Keul, Ute Koczy, Kerstin Müller (Köln), Lisa Paus, Claudia Roth (Augsburg), Manuel Sarrazin, Dr. Frithjof Schmidt, Hans-Christian Ströbele und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Cyber-Strategie der Bundesregierung – Militärische und verteidigungspolitische Aspekte

Die „Cyber-Sicherheitsstrategie für Deutschland" der Bundesregierung vom Februar 2011 betrachtet den Schutz des Cyber-Raums als existentielle Frage des 21. Jahrhunderts. Um Sicherheit im Cyber-Raum zu gewährleisten, strebt sie eine enge internationale Zusammenarbeit an und hebt hierbei insbesondere die NATO hervor. Nach Behördenangaben und Meinung von Expertinnen und Experten hat die Bedrohung des Cyber-Raums in jüngster Zeit zugenommen und mit neuen, insbesondere staatlichen Akteuren eine neue Qualität erreicht. Als eine Antwort darauf wurde am 16. Juni 2011 das Nationale Cyber-Abwehrzentrum vom Bundesministerium des Innern eröffnet, mit dem künftig schneller auf Angriffe reagiert und das Krisenmanagement optimiert werden soll.

Es gibt berechtigte Zweifel, ob die Strategie der Bundesregierung und das neue Cyber-Abwehrzentrum geeignet sind, die Sicherheit des Cyber-Raums in Deutschland zu verbessern. Es fehlt an technischer Expertise und Ressourcen, um komplexe und gefährliche Angriffe überhaupt zu erkennen und darauf zu reagieren. Auch die militärischen und verteidigungspolitischen Aspekte von Internetsicherheit in Deutschland bleiben diffus. Dabei basieren laut Cyber-Strategie der Bundesregierung die hochtechnisierten Formen des Krieges im Informationszeitalter „auf einer weitgehenden Computerisierung, Digitalisierung und Vernetzung fast aller militärischer Fähigkeiten".

In Bezug auf die Gefährdungslage und Cyber-Sicherheit in der Bundeswehr fragen wir daher die Bundesregierung:

1. Welche über das Krisenmanagement und die Fähigkeit zur Angriffserkennung und Schadensbekämpfung hinausreichende Aktivitäten im Bereich Cyber-Sicherheit gibt es innerhalb der Bundeswehr?
2. Inwiefern führt die Bundeswehr Angriffssimulationen im Cyber-Raum durch?
3. Inwiefern führt die Bundeswehr auch über die eigenen Systeme hinausreichende Aufklärungsaktivitäten durch?
4. Welche Forschungsaktivitäten gibt es?
5. Inwiefern führt die Bundeswehr auch Maßnahmen zum Aufbau offensiver Fähigkeiten durch?

6. Welche über das Krisenmanagement und die Fähigkeit zur Angriffserkennung und Schadensbekämpfung hinausreichende Aktivitäten im Bereich Cyber-Sicherheit gibt es innerhalb des Bundesnachrichtendienstes?
7. Inwiefern führt der Bundesnachrichtendienst Angriffssimulationen im Cyber-Raum durch?
8. Inwiefern führt der Bundesnachrichtendienst auch über die eigenen Systeme hinausreichende Aufklärungsaktivitäten durch?
9. Gibt es Forschungsaktivitäten, und wenn ja, welche?
10. Gibt es Maßnahmen zum Aufbau offensiver Fähigkeiten, und wenn ja, welche?
11. Inwiefern bedient sich die Bundeswehr im Rahmen von Auslandseinsätzen besonderer Cyber-Fähigkeiten, für deren Vorhaltung bzw. Anwendung ein Mandat des Deutschen Bundestages erforderlich ist?
12. Inwieweit wurde in der Vergangenheit bei Auslandseinsätzen der Bundeswehr bereits auf Fähigkeiten der Bundeswehr im Bereich des elektronischen Kampfes im bzw. aus dem Cyber-Raum zurückgegriffen?
13. Inwiefern ist die Abteilung Computer und Netzwerkoperationen (CNO) in der Tomburg-Kaserne in Rheinbach, die dem Kommando Strategische Aufklärung unterstellt ist, die einzige Dienststelle der Bundeswehr, die für den Bereich Cyber-Sicherheit sowie den elektronischen Kampf im Cyber-Raum abgestellt ist?
14. Inwiefern berät die Abteilung CNO Stellen der Bundesregierung wie das Bundesamt für Sicherheit in der Informationstechnik, das Bundesministerium des Innern oder aber das neu eingerichtete Nationale Cyber-Abwehrzentrum?
15. Welchen konkreten Auftrag hat die Abteilung CNO, und welche rechtliche Grundlage gibt es für ihre Arbeit?
16. Welche Kooperationen der Bundeswehr mit den Streitkräften anderer Staaten existieren im Bereich Cyber-Security, und welcher Natur sind diese Kooperationen im Einzelnen?
17. Welche Ergebnisse zeitigte die jeweilige bilaterale Zusammenarbeit in Bezug auf Cyber-Security mit den USA, Frankreich, Großbritannien und der Schweiz?
18. Was sind Inhalt und bisherige Ergebnisse des seit November 2010 stattfindenden Dialogs mit den USA (Cyber Command beim US-Militär und Fort Meade bei der National Security Agency)?
19. Was sind Inhalt und bisherige Ergebnisse des Erfahrungsaustausches unter Regierungsressorts mit der Schweiz im Bereich Cyber-Sicherheit?
20. Welche Organisationen stehen für die Bundeswehr bei der internationalen Kooperation im Bereich Cyber-Sicherheit im Mittelpunkt?
21. Welche Anstrengungen zur internationalen Kooperation unternimmt die Bundeswehr mit welchen Ergebnissen im Rahmen der EU, insbesondere der Gemeinsamen Sicherheits- und Verteidigungspolitik?
22. Welche Implikationen hat die Beschreibung des Cyber-Raums im Cyber-Bericht der Bundeswehr als 5. Operationsdimension für die Mandatspflicht von Cyber-Operationen seitens der Bundeswehr?

Berlin, den 18. August 2011

Renate Künast, Jürgen Trittin und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333